CLAIMS

What is claimed is:

1. A method, comprising the computer-implemented steps of:
receiving trust information defining one or more trusted signatories;
receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives;
attempting to verify the one or more digital signatures based on the trust information;
applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

2. A method as recited in Claim 1, further comprising the steps of:
verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host.

3. A method as recited in Claim 1, further comprising the steps of:
receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;
applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

4. A method as recited in Claim 1, further comprising the steps of:
receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;
applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

5. A method as recited in Claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host.

6. A method as recited in Claim 1, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures.

7. A method as recited in Claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures.

8. A method, comprising the computer-implemented steps of:

receiving trust information defining one or more trusted signatories;

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

9. A method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in memory.

10. A method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of:

generating a secure hash of the one or more configuration directives;

determining if the secure hash is found in non-volatile memory.

11. A method as recited in Claim 8, further comprising the step of storing the secure hash in non-volatile memory, in association with an expiration value, when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period.

12. A method as recited in Claim 8, further comprising the steps of:

verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host.

13. A method as recited in Claim 8, further comprising the steps of:

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

14. A method as recited in Claim 8, further comprising the steps of:

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures.

15. A method as recited in Claim 8, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host.

16. A method as recited in Claim 8, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures.

17. A method as recited in Claim 8, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures.

18. A method for verifying configuration changes for network devices using digital signatures, comprising the computer-implemented steps of:

receiving a public key for a user of the network devices;

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device;

receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date-time value;

determining if the date-time value is within the time period;

determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; and

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, performing the steps of:

attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures,

and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

19. A method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

20. A method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

21. A computer-readable medium carrying one or more sequences of instructions for verifying configuration changes for network devices using digital signatures, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving trust information defining one or more trusted signatories;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives;

attempting to verify the one or more digital signatures based on the trust information;

applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

22. A computer-readable medium as recited in Claim 21, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of any of Claims 2, 3, 4, 5, 6, or 7.

23. A computer-readable medium as recited in Claim 21, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

24. A computer-readable medium as recited in Claim 21, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

25. An apparatus for verifying configuration changes for network devices using digital signatures, comprising:

means for receiving trust information defining one or more trusted signatories;

means for receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives;

means for attempting to verify the one or more digital signatures based on the trust information;

means for applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

26. An apparatus as recited in Claim 25, further comprising means for performing the steps of any of Claims 2, 3, 4, 5, 6, or 7.

27. An apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

28. An apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.

29. An apparatus for verifying configuration changes for network devices using digital signatures, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving trust information defining one or more trusted signatories;

receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives;

attempting to verify the one or more digital signatures based on the trust information;

applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

30. An apparatus as recited in Claim 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of any of Claims 2, 3, 4, 5, 6, or 7.

31. An apparatus as recited in Claim 29, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

32. An apparatus as recited in Claim 29, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature.